Office de la propriété intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An Agency of Industry Canada

Bureau canadien des brevets
Certification

Canadian Patent Office
Certification

La présente atteste que les documents ci-joints, dont la liste figure ci-dessous, sont des copies authentiques des documents déposés au Bureau des brevets.

This is to certify that the documents attached hereto and identified below are true copies of the documents on file in the Patent Office.

Specification and Drawings, as originally filed, with Application for Patent Serial No: **2,392,326**, on July 3, 2002, by **NEWTRAX TECHNOLOGIES INC.**, assignee of Alexandre Cervinka, Solange Mai-Xuan, Yvan Castilloux and Vincent Kassis, for "Monitoring System and Method".

CERTIFIED COPY OF PRIORITY DOCUMENT

Agent certificateur/Certifying Officer

July 9, 2003
Date

Canada

(CIPO 68)
04-09-02

OPIC CIPO

ABSTRACT

Mobile station protocol that allows mobile stations to send data to cellular networks even if a jammer is blocking all land station to mobile station communication. The end result is a best-effort uplink communication service. The mobile station sends a plurality of times the same data-holding frame over all possible access channels to the network.

Central server using artificial intelligence and stochastic models to track a remote mobile client equipped with inertial sensors and whose movement is constrained by a set of possible routes on a digital map. A mobile terminal starts by sending to the remote server its initial position and orientation, and then continuously sends to the remote server data kinetic parameters obtained from inertial sensors. Temperature and other parameters needed to tune pre-defined stochastic models can also be sent to the server on an as-needed basis. The server software compensates for all non-ideal and induced errors to the received data, extracts various information from the corrected signals, applies the digital map constraints, and provides the tracking user with the possible routes.

BACKGROUND OF THE INVENTION

Technologies such as GPS and existing cellular radio links have constraints that create major vulnerabilities in existing tracking systems. Thieves have learned how to exploit these vulnerabilities to disable systems within a few seconds.

The technologies NewTraX has developed opens new possibilities for the design of tracking systems:

- Allow the recovery system to work even if thieves use jammers[1].
- Increase the options for placement/concealment of tracking module.
- Remove the line-of-sight requirement between antenna and satellites.

NewTraX took advantage of the new possibilities offered by its technologies to add significant hurdles to the process thieves must go through to disable the tracking system. The methods used by thieves to disable existing tracking systems are:

1. **Cellular jamming:** All tracking solutions on the market today are vulnerable to cellular jamming. Cellular jammers are commonly used since 1998 to control cellular phone usage in certain areas such as churches or theatres. Go to www.mobileblocker.com to order a jammer online. NewTraX has developed the only jamming-resistant cellular link to work over existing commercial networks. No change to network infrastructure is necessary.
2. **GPS jamming:** All commercial GPS-based services on the market today are vulnerable to GPS jamming. However, GPS jammers are not available to the general public because all possible applications are necessarily ill-purposed. Although simple in design, GPS jammers were feared by industrialized nations because they could seriously jeopardise the effectiveness of many modern weapons such as aircrafts and missiles often guided by GPS. A Russian company named Aviaconversia[2] used to sell GPS jammers for 4000$US. NewTraX's solution is unaffected by jamming of GPS.
3. **Finding and destroying the tracking module or antenna:** All GPS-based systems require an unobstructed line of sight between the GPS antenna and the GPS satellites. This constraint requires the GPS antenna to be installed in specific locations on the roof of the trailer, and these locations are well known by thieves. NewTraX's cargo recovery system is based on inertia, which can be sensed from any position on the trailer, on the pallet or even on the cargo itself. NewTraX's tracking module can therefore be installed randomly anywhere in the trailer, which represents an area exceeding 2000 square feet. This means that information shared among thieves pertaining to the location of the device

[1] Jammers are electronic devices that create interference on communication channels.
[2] http://www.info-sec.com/denial/denial_012298a.html-ssi

is useless: the procedure used to determine the position of the tracking module must be repeated every time.

4. **High-power electro-magnetic field to "grill" all electronics within a given range:** All the electronics in NewTraX's tracking module are within a faraday cage. No electro-magnetic field can enter the cage.
5. **Induced power surge on trailer power bus:** NewTraX's tracking module is protected from such an attack by a large decoupling capacitor combined with a fuse.

For instance, it is well known in the trucking industry that thieves easily disable GPS based tracking systems. All GPS based systems require an unobstructed line of sight between the GPS antenna and the GPS satellites. This constraint requires the GPS antenna to be installed in specific locations on the roof of the trailer, and these locations are well known by thieves.

Newco's cargo recovery system is based on inertia, which can be sensed at any point on the trailer. Newco's tracking module can therefore be installed randomly over an area exceeding 2000 square feet. This means that information shared among thieves pertaining to the location of the device is useless: the procedure used to determine the position of the tracking module must be repeated every time.

This is an example of how Newco took advantage of the new possibilities offered by its technology to add significant hurdles to the process thieves must go through to disable the tracking system.

There are several significant problems with using cellular based positioning technologies for our applications:

1. Different network operators are deploying different position determination technologies. These technologies might represent an interesting option for applications where coverage is limited to a single network, but will not work if application requires roaming between networks. Roaming is a pre-requisite to a NAFTA-wide application.
2. Roll-out of technologies has been delayed[3], and availability of service will be limited to urban areas at first.
3. The leading technology is by far A-GPS, developed by Snaptrack[4]. This technology, is based on GPS, and retains many of the GPS constraints that limit the development of a robust tracking system in a hostile environment.
4. Boomerang uses Cell ID technology (figure YYY). The limited precision of this technology forces Boomerang to send employees with special equipment in the approximate area to determine the exact position. The inherent delays in this recovery process make the solution unsuitable for

[3] The Enhanced-911 mandate from the FCC to U.S. operators initially required operators have the capability of locating customers by October 2001, but with the economic downturn and loss of hype about location-based services, most operators have requested additional time.

[4] http://www.snaptrack.com/

cargo recovery, and intervention of a vehicle with employees considerably limit the scalability of the service.

Mechanical inertial sensors have been available since the end of the Second World War. *Inertial navigation systems* (INS) based on mechanical inertial sensors are used in civil and military aviation, cruise missiles, submarines and space technology. For these areas of operation, the components used and the entire system must be very precise and reliable. The cost of these systems is very high and their large size make them unsuitable for applications such as automotive or consumer electronics.

The latter applications require very small size and inexpensive implementation. Recently, 'solid state' solutions have been realized by using only discrete integrated electro-mechanical or electro-optical sensors. Industrial demand for low-cost sensors (car airbag systems) and recent progress in MEMS[5] integration technology lead to sensor products, which are small (single chip) and inexpensive (~15 US$).

Newco's remote error correction algorithms would be an overkill for inertial navigation systems based on high-end mechanical inertial sensors.

CDMA[6] is a spread spectrum technology that was initially developed by the U.S. military to protect wireless communications from jamming.
Traditional narrowband communications can easily be jammed because the frequency used as a communication channel can easily be detected and jammed. Narrowband communications create a power peak above the noise floor on the channel frequency, and a spectrum scanner can easily detect this peak.
CDMA spreads the signal power across a wide band below the noise floor. This makes it impossible for a spectrum scanner to detect which frequency band is being used as a communication channel. Without knowing which radio band is used, it is a lot harder for the enemy to jam the channel. The only option is to guess or jam the entire RF band (would require an incredible amount of power).
In a commercial context, the frequency bands used by cellular network operators are well known, so CDMA based networks are as vulnerable as their narrowband counterparts. The commercial jammers available today block CDMA based cellular communications.

Vehicle recovery companies

There are many new entrants in this market, most using a GPS/Cellular combination. Although vehicle recovery is the main focus, they are increasingly combining their basic service with other information and security services.

---

[5] Micro Electro-Mechanical System. Please refer to appendix YYY for a January 31st 2002 article on the future of MEMS.
[6] Code Division Multiple Access

Boomerang

Boomerang Tracking Inc., founded in 1995, is a public Canadian company headquartered in Montreal, Quebec. The company has 90 employees. An early entrant in the stolen vehicle recovery service, Boomerang's main strength is brand name and effective marketing. The company innovated with its strategy of convincing insurers to decrease insurance premiums of Boomerang clients (although Boomerang is now not the only one to offer this advantage.) Boomerang targets mainly users of at-risk cars. Furthermore, it has just signed a partnership with Cingular in the US, and is expected to focus on capturing the US mass-market. Although their most recent solution "Boomerang 2" is a significant improvement over the first solution, it still has some significant flaws for the cargo recovery application:

- **Boomerang 2 is not designed for a tractor-trailer configuration, and is unable to automatically detect a trailer theft:** designed for "one piece" vehicles such as cars or heavy-duty equipment. The Boomerang 2 is activated if the transponder attached to the customer's key chain is not present when the car is started. The Boomerang tracking unit must be installed in the trailer since 80% of trailer thefts in Newco's target market are done using stolen tractors. Boomerang has integrated its transponder reader with its tracking unit, and there is no easy procedure by which the trucker could place the transponder tag near the transponder reader in the trailer. This is one of the reasons why they do not use Boomerang 2 with trailers.
- **Boomerang 1, which is used for trailers is vulnerable to jamming:** with Boomerang 1, the owner must call the Boomerang headquarters to report the theft, so the monitoring staff can activate the Boomerang by sending a command signal through the cellular network. The downlink is vulnerable to jamming, so if the thief uses a jammer, the Boomerang will be unable to receive the command signal, so will never enter "tracking mode".
- **Real-time tracking is not possible:** must send one or more persons in a « tracking vehicle » to the cell area to be able to locate the stolen car.
- **Intervention of a "tracking vehicle" too costly for use of position determination technology in any trailer fleet management application:** cells in a cellular network often have several kilometres of radius. "Cell ID" position information is not sufficient for trailer fleet management applications. Newco's solution can provide precise real-time position information to trailer fleet management applications. This will be an important factor for big fleet management players seeking to purchase a company specialized cargo recovery.
- **Cellular technology used requires frequent communication with cellular network, which drains the battery:** trailers are often left unattended in lots for several days, even weeks, without being plugged into some sort of power source. Power consumption is critical in

standby mode. This is another major reason why Boomerang does not install its units in the trailers.

- **Recovery area does not include Mexico, and in order to recover a stolen vehicle in the U.S., Boomerang must send a person with special equipment in the approximate area in order to determine the exact position:** for fast recovery Boomerang will use planes or helicopters.

In a press release from October 18th 2001, the company mentioned **"Boomerang2 is a proprietary device that will only be installed in passenger vehicles and trucks in the first phase of its launch."**[7]

LoJack

LoJack, a long time player in the vehicle recovery industry, entered the market with its patented technology in Massachusetts in 1986. In 1989, as LoJack expanded to other states, the Federal Communications Commission allocated a police radio band for the Stolen Vehicle Recovery Network, allowing the LoJack technology to operate nationwide.

The LoJack System is always in the receiving mode. . If the vehicle is stolen, the filing of a stolen vehicle report to the police will automatically activate the LoJack System in the vehicle. The LoJack System will then transmit a silent signal to Police Tracking Computers (Figure 1). Many police cars as well as police aircraft in LoJack coverage areas are equipped with LoJack Police Tracking Computers.

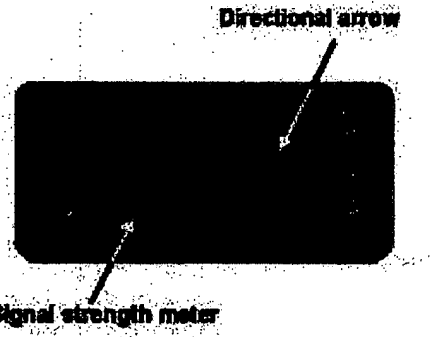


Figure 1: *LoJack handheld computer provided to many police officers in the U.S.*

Using the directional arrow and strength meter on the police-tracking computer, a patrol officer can track the origin of the signal, i.e. the stolen vehicle.

- **Coverage limited to high-crime rate metropolitan areas in certain states only.**

[7] http://biz.yahoo.com/cm/011018/yytpwpc6uxj8ye9_micpdw_1.html

- **Service not available in Canada:** the police radio band for the Stolen Vehicle Recovery Network has not been created by the CRTC.
- **Impossible to remotely determine if device is working, must get an inspection done at local LoJack office:** the LoJack device is tested and certified to be in working condition at the time of installation. After that, the company recommends an inspection be done every two years. If the customer believes the unit requires service, the only way to find out is to visit the local LoJack office.
- **Receiver used for device activation vulnerable to jamming, the device could never change to alarm mode:** same problem as with Boomerang 1, the device is triggered through the downlink of a wireless network.
- **Real-time tracking is not possible:** the device never transmits any information, it can only radiate on a given frequency to signal its presence to patrol officers.
- **Undetermined response time:** once the customer has reported the theft and the device is activated, no one knows where the vehicle is. The system depends on patrol officers throughout the coverage area to pass near the stolen vehicle and detect with their LoJack handheld computer the presence of a stolen vehicle.

Vigil

Subsidiary of Adastra, a contract manufacturer of electrical systems, Vigil's solution is essentially a traditional GPS/cellular-combination device. Vigil's solution has been commercially available since May 2001. Vigil is currently focusing on the consumer market, but also offers custom solutions for commercial fleets. Their differentiation factor is the integration of telematic functionality such as remote door locking/unlocking with their anti-theft solution. Vigil's main strength is a privileged relationship with an electrical systems manufacturer. We estimate its size to be 12 employees, including 6 engineers. **The solution it currently proposed has some serious flaws for any application taking place in a hostile environment**, but it remains to be determined how much work would be required for them to adjust their offering:

- The localization technology is GPS, which makes their solution vulnerable to GPS-jamming. The antenna must also be placed near the roof's surface. If the antenna is found and destroyed, there is no other way to locate the vehicle.
- The Vigil system is triggered via the tractor's standard alarm system. When it is installed on the trailer, **the driver must manually arm** and disarm the system. This makes their system vulnerable to internal collaboration with thieves. The tractor's system could also be managed remotely, but, based on the communications requirements this would incur high operating costs.
- The communication technology used by Vigil (Aeris.net) is vulnerable to jamming.

***Trailer* fleet management companies**

The following companies do trailer tracking for the "trailer fleet management" application, which is projected to represent a large and growing market. **These companies are not in direct competition with Newco since their solutions are not designed to withstand a hostile context.**

There are many company's offering trailer-tracking products. They integrate a GPS receiver with some sort of cellular modem in a main module. The main module is hidden in the walls of the trailer, and a GPS/cellular antenna hidden on the roof of the trailer is connected to the main module using a long antenna cable (figure 2). The "covert" antenna is placed in the marker lights on top of the trailer or a hole covered with fibreglass (figure 3).

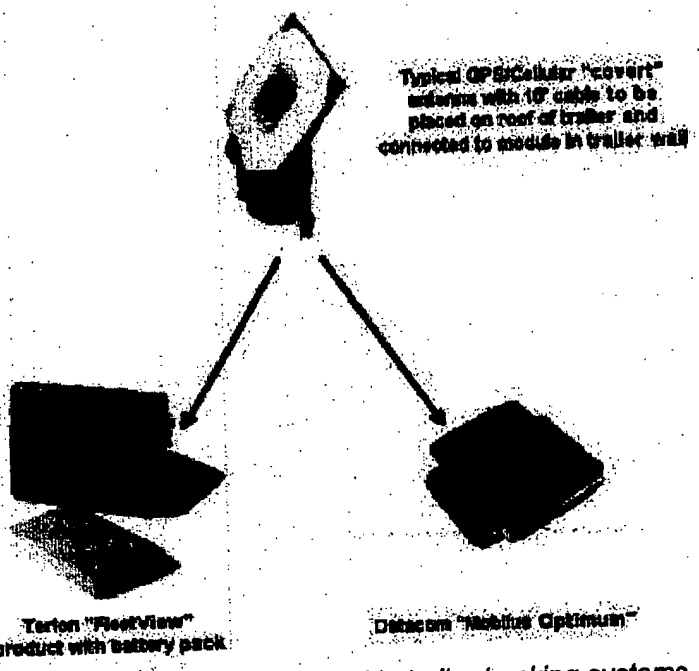


Figure 2: GPS antenna used in trailer-tracking systems

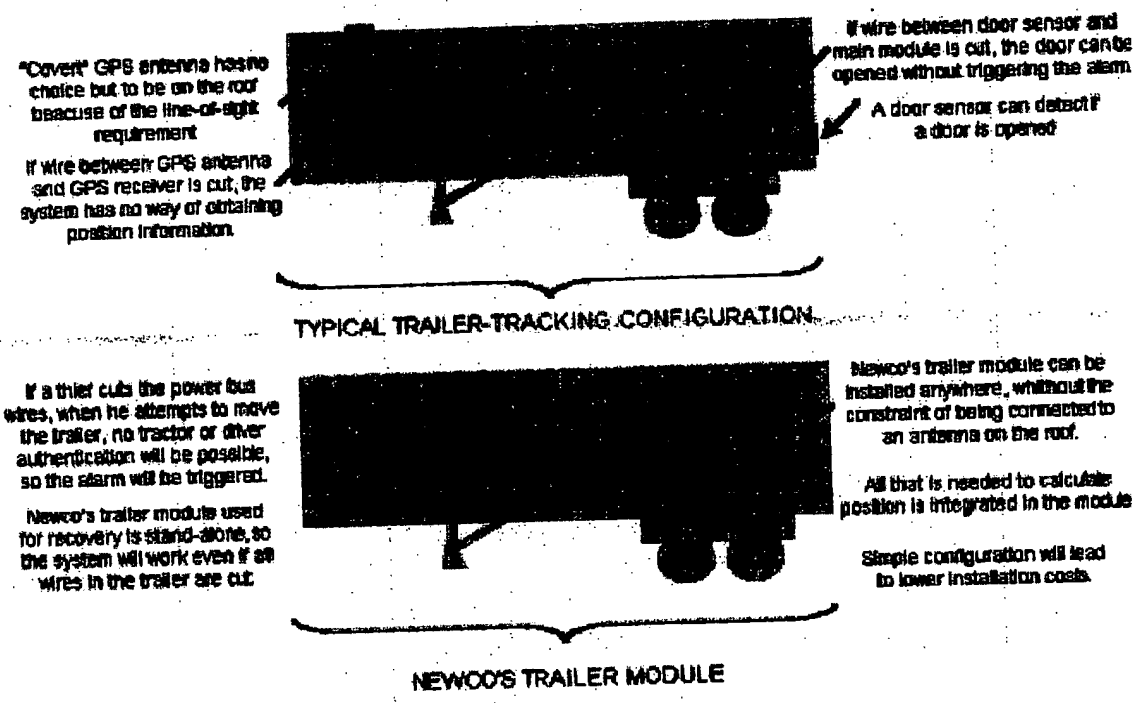


Figure 3: Typical trailer-tracking offering compared with Newco

Although their focus is on trailer use management, trailer-tracking systems can also offer some security features:

1. Monitor trailer motion and door sensor.
2. Notify dispatcher when trailer movement or door opening has violated lockdown.
3. Enter continuous interval tracking mode automatically and pages or emails notification to security personnel.
4. Geofencing allows to specify an authorized area within which the trailer is authorized to travel.

Terion

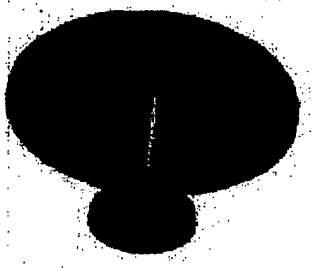
"Terion is focusing its product development and business strategy toward meeting the needs of transportation, heavy equipment, and service fleet markets in the NAFTA trade region, followed by additional domestic and international markets."[8]

- **If used as a theft detection system, affects/changes carrier's operations considerably:** For instance, in order to protect the cargo, the carrier must specify that between 7 PM on Thursday the 21st of March and 8 AM on the 22nd of March the trailer should not move, have its doors open, or cargo loaded/unloaded. Theoretically, such a system would work, but it is very complex to implement since the carrier is not aware of all trailer related activities such as when the driver takes a break, or at what time he will start driving, when will the trailer be moved within a lot or at the customer's premise, or when a partial load will be added to a "Less Than Truck Load" shipment.
- **Manual setting of sensor based triggers for alarm through the web entail heavy communication costs:** a service charge of 20$/month includes 30 communications with the trailer. Each additional communication cost 65 cents. Setting an alarm would cost one communication, deactivating an alarm another. If a single alarm was activated/deactivated every day, this would represent 30 communications per month, and that is without using any of the "trailer fleet management" features for which the product is designed! Forced by financial considerations, the carrier would have to limit the times he decides to protect his cargo. The choice of how to set the alarm is already difficult enough since the carrier is not fully aware of the trailer activities, any trucker could be corrupt, and any type of cargo from soap to aluminium can be stolen.
- **Theft detection mechanism requires honest employees:** a large proportion of cargo thefts are accomplished with the help of an insider accomplice. The carrier will depend on the input from his employees in order to properly set the triggers for the alarm. For instance, if the driver reports he will be driving from 8 AM to 6 PM, then the motion

[8] From company press release

sensor will be deactivated as of 8 AM...the driver is aware of this, and could advise a thief to take off with the truck at 8:02 AM.

- **Could not be used on container trailers (chassis):** the FleetView control unit is mounted inside the trailer wall, and the GPS antenna, which requires line of sight with the satellites, must be mounted somewhere on the roof (Terion installs the antenna in the marker lights on the roof). **No GPS based solution can work with containers since no GPS antenna can be mounted on a container chassis and have line of sight with the satellites.**
- **Thieves easily disable satellite-based tracking systems[9], and no backup system to GPS is included:** GPS is vulnerable to jamming, and because of the line of sight requirement between the antenna and the satellites, the places where the antenna can be concealed on the roof are limited, and thieves easily find them, break them, or simply cover them with aluminium foil.
- **Cellular technology used is vulnerable to cellular jamming:** cellular jammers are commercially available for as low as 150$, and can block all attempts to transmit position information[10]. Terion uses the WIN[4] network.
- **The tractor sensor available from Terion does not actually detect if a tractor is attached, but rather detects if the trailer is plugged into a power source:** there are many reasons why a carrier may want to know if the trailer is plugged into a power source, for instance in the case of a refrigerated trailer used to store meat. However, it is not very reliable to detect theft.
- **Terion will offer in the future an option to use the Wabash[11] sensor integrated in the kingpin of new Wabash trailers to detect if a tractor is actually attached:** this system could easily be used to offer tractor authentication, but a completely different approach would be needed to extend the feature to include driver authentication. The Wabash sensor is not available on all legacy trailers, and in the future will only be available on Wabash trailers. Legacy trailers cannot take advantage of this sensor because complex modifications requiring among other things drilling holes in the key-pin would be necessary.



[9] Well known in the industry, and stated in http://www.chicagofed.org/bankinforeg/bankregulation/archives/article0212ln.cfm

[10] http://www.mobileoffice.co.za/accessories/phone_blockers/mobileblocker.htm provides an example of commercially available jammers. Since professional thieves will use "high-tech" tools to disable our system, we must have jamming-resistant connectivity.

[11] Largest trailer manufacturer in the U.S. : http://www.wabashnational.com/

Figure 4: Kingpin used to join trailer with tractor

- **No support is offered to manage efforts for cargo recovery. When the carrier receives an alarm through the web, it is up to him to take action.**

Datacom

Datacom is a private company marketing products and systems for the automated management of vehicle fleets. Founded in 1999 by Paul-André Savoie, who also founded Boomerang, the company currently employs 35 people. Situated in Laval's Technoparc, its main strengths are its board of directors (includes Jacques Duchesneau and Frank McKenna) and a partnership with Manac a local trailer vendor. The system is very similar to Terion's product, so suffers from the same weaknesses for the cargo recovery application:

- **If used as a theft detection system, affects/changes carrier's operations considerably.**
- **Manual setting of sensor based triggers for alarm through the web represents prohibitive communication costs.**
- **Theft detection mechanism requires honest employees.**
- **Could not be used on container trailers (chassis).**
- **Thieves easily disable satellite-based tracking systems[12], and no backup system to GPS is included**
- **Cellular technology used is vulnerable to cellular jamming: Datacom uses the Aeris.net network.**
- **No support is offered to manage efforts for cargo recovery. When the carrier receives an alarm through the web, it is up to him to take action.**

Tractor fleet management companies

"These AVL systems can pinpoint a tractor anywhere, at any time and exchange information with it and the driver, interface with corporate GIS mapping and vehicle dispatch systems, offer on-line vehicle diagnostics, etc. All good stuff, but when the tractor leaves the trailer, the trailer and it's cargo virtually "vanish"...obviously, a huge gap exists to any carrier wanting to know where his trailers and cargos are after the tractors disconnects from it!"[13]. Examples of such companies are Girit Canada, AirIQ, Cadec.

In conclusion:

First, all the systems on the market today are easily disabled by thieves within seconds. For example, the new trend in thefts is the use of jammers. A jammer is an electronic device that creates interference on communication

[12] Well known in the industry, and stated in http://www.chicagofed.org/bankinforeg/bankregulation/archives/article0212ln.cfm
[13] From the letter of validation from Roger Smith

channels. Today, thieves use jammers to disable all tracking systems within seconds, including Boomerang and CDMA based channels.

Second, GPS technology cannot be used to determine the position of cargo if the cargo is stored indoors, in a trailer, or in a container: GPS technology requires an unobstructed line-of sight between the antenna and satellite. Moreover, GPS is not effective in tracking stolen trailer because thieves easily break the GPS antenna installed on the roof.

Third, systems like Boomerang have a consistent track record for finding empty trailers. When a theft occurs, Boomerang only knows the approximate position of the stolen trailer within several kilometers. An employee with special equipment must be sent in the approximate area to determine the exact position. The cost and delays inherent to this procedure make a system like Boomerang unsuitable for an application such as cargo tracking and recovery. Boomerang's technology is great to recover vehicles since finding a stolen vehicle 24 hours after the theft is considered a success. However, finding a stolen trailer 3 hours after the occurrence of a theft means finding an empty trailer with the cargo gone.

APPLICATIONS AND MARKETS:

Organizations that transport potentially dangerous cargo must take all necessary precautions so their cargo does not get in the hands of terrorist or professional thieves. Existing systems used to monitor cargo in transit have the following weaknesses:

1. Vulnerable to GPS[14] and cellular[15] jamming
2. Only track vehicles across NAFTA – not cargo initially in the vehicles
3. Cannot detect unauthorized unloading and other types of thefts

Other applications and markets for NewTraX technology could be:

1. Professional thieves often target companies that produce and transport easily resellable high-value goods such as cigarettes, alcohol, and electronics. The American Association of Insurance Services (AAIS) reported that cargo theft is estimated to cost Americans some $4 billion to $6 billion a year and that it adds $100 to the cost of every personal computer shipped in the U.S.[16]
2. The new trend in home monitoring such as the "Alarm Force"[17] service is wireless connection that allows the central monitoring center to be notified even if thieves cut the phone line. These systems are vulnerable to off-the shelf jammers that can be ordered online for less than 500 $US[18]
3. Intelligence services such as the CIA use modified cellular terminals as eavesdropping bugging devices. With the advent of commercially available jammers this capability is compromised.

---

[14] http://www.info-sec.com/denial/denial_012298a.html-ssi
[15] http://www.ziplar.com/p/products/others/electronics/jammer/jammer.html
[16] http://www.aaisonline.com/communications/viewpoint/vp24_2.htm
[17] http://www.alarmforce.com/alarmplus.html
[18] http://www.mobileblocker.com/

DESCRIPTION OF THE PREFERED EMBODIMENT

Cellemetry's modifications to the TIA-553 were to create an uplink data channel through the autonomous registration procedure. More specifically, the modifications are:

1. Replacing the Electric Serial Number with 32bits of data
2. Forcing the autonomous registration to occur when the application software has data to send.

NewTraX's additional modifications to the TIA-553 (mobile station side only) are to create a jamming-resistant uplink between the mobile station and the land station.

General concept

The mobile station uses the jamming-resistant uplink only if the application software detects a hostile environment (for instance a theft has been detected). The moment in time where a hostile environment is detected is referred herein as the "event".

The time period before the "event" is referred herein as the "pre-event" period.
The time period after the "event" is referred herein as the "post-event" period.

The post-event period is assumed to last no more than 3 hours.
During the post-event period, the mobile station is assumed to remain within the coverage of the network detected by the mobile station just before the event.

During the pre-event period, the mobile station acts as a standard Cellemetry terminal, but it must keep in memory the following variables it has received over the FOCC of the dedicated control channels or paging channels:

- N: Number of paging channels in the system
- CPA: Combined paging/access field
- CMAX: Number of access channels in the system
- NEWACC: New Access Channel

Once an event is detected, the mobile station stops updating the values of the abovementioned parameters based on the overhead messages received from an FOCC.

The first and last access channels are determined using the standard equations:
If mobile station on A-band system (B band case uses similar procedure):

If paging and access channels are combined (CPA = 1), set FIRSTCHA to the first dedicated control channel on System A:

- 834.990 MHz mobile Tx, 879.990 MHz land Tx

...and the last access channel (LASTCHA) to:

- LASTCHA = FIRSTCH - CMAX + 1

If paging and access channels are not combined (CPA = 0), set FIRSTCHA to the first dedicated control channel on System A minus N x channel bandwidth:

- (834.990 - N x 0.030) MHz mobile Tx, (879.990 - N x 0.030) MHz land Tx

...and the last access channel (LASTCHA) to:

- LASTCHA = FIRSTCH + CMAX - 1

If NEWACC specified, set

- FIRSTCHA = NEWACC
- LASTCHA = NEWACC - CMAX + 1

If used in a mobile application (for instance telematics), the mobile station transmits the registration frame [(LASTCHA-FIRSTCHA+1) x 4] times, i.e. once on each possible RECC with all four digital color code (DCC). Typically, the network should receive only three frames since there should only be an average of three neighboring land stations.

If used in a fixed application (for instance home alarms), the mobile station transmits the registration frame only on the three strongest RECC access channels with corresponding DCC. Since the mobile is not moving, it should always remain in the coverage of the same neighboring land stations.

One possible implementation where the "event" is the absence

First modification for increased bandwidth

Basic Cellemetry uses a single MIN to make the registration request. The MIN and ESN is forwarded to the Cellemetry server on the IS-41 (inter-cellular) network, where the encapsulated data is received, and a "reject registration request" message is sent back to the host network, and the host network then deletes the record from the VLR. The loop can take as much as 1 minute to complete, and the terminal with the same MIN is unable to send an additional registration request. This system would offer a 32bit/minute bandwidth.

To increase the bandwidth, NewTraX uses MIN rotation.
Given the following constraints:

Ø The RECC bit stream is at a 10kbit/s.

Ø An autonomous registration frame is 768bits (because of redundancy)

Ø A time window must be open for other AMPS terminals to complete their normal control exchange to obtain a voice channel.

Ø There is a parameter in the mobile station called BIS that identifies whether a mobile station must check for an idle -to-busy transition on the RECC when accessing a system. This is a value that is stored in mobile stations and that cannot be determined pre-event by listening on the forward control channels. Worst case must be assumed, i.e. that other terminals will attempt to communicate without checking the busy/idle state. Collision probability must be taken into account. NewTraX system makes sense based on the assumption that the RECC channels are seriously underutilized. A mobile station with the BIS enabled will

One possible implementation is that NewTraX adds 180 slave MIN to every mobile station in addition to the MIN used to uniquely identify the terminal.

If a registration request carrying a new 32bit data packet is sent over all access channels simultaneously and with all four digital color codes sequentially every 308 ms using a different MIN, then a bandwidth of 100bits/s can be achieved. However, 180 records will be continuously added/deleted to the VLR, and the communication will occupy almost all the available bandwidth over the RECC.

Second modification to increase bandwidth

Consider a cellular network with j access channels. In order to maximize the likelihood of network reception of the autonomous registration request under jamming conditions, the terminal must transmit sequentially in time j copies of the autonomous registration request, once over each access channel. Since a single frame is 768 bits and each access channel has a bandwidth of 10 000bits per second, a single transmission over a all access channel takes over (0.07seconds x j access channels x 4 digital color codes).

In order to increase the bandwidth of the jamming-resistant data uplink by a factor j, NewTraX uses multichannel modulation to enable the mobile station to radiate on all j access channels simultaneously in time.

Please refer to figure YYY

For the analog implementation, unless prior information is known on the Cellemetry partner network, the frame must be sent on the 21 RECC of both A & B bands, repeated for each colour code in order to insure that the information on the frame will be received by the Cellemetry server.

We know that we cannot find a way around time slots for frames, or codes.
However we could get a receiver with a 10% error margin on the symbol timing to accept a frame if this frame was sent 10 times with phase shifts of (symbol period/10)

These modifications can also apply to cellular networks with similar access concepts such as IS-95 ,NMT, etc.

OVERALL TRACKING SYSTEM

The land inertial navigation system (INS) has two distinct software modules: the data-analysis module containing integration and gesture-matching algorithms, and the map-matching module. These two modules will be described in more details below. The route data is stored on a server along with the data-analysis and the map-matching programs. The inertial sensors are separated in space and sends the measured signals wirelessly to the server via a Cellemetry anti-jamming transponder.

The data-analysis module obtains the information of an external aid to obtain the initial position, computes a displacement and detects gestures from the data measured from inertial sensors. The map-matching module, which is based on a stochastic model, displays a set of positions with each having a probability.

Remarks

1. The (INS) only uses an external aid other than map-matching for the initial absolute coordinate. That is, only the measured signals from the sensors are used to compute a displacement and detect gestures. Conventional land INSs are used as a complementary tool when GPS is not available. They are used in automobiles in order to give the precise location of the vehicle on a map. Hence, they have very stringent location precision requirements (within one meter). Our system rather outputs the possible routes taken by the vehicle and a probability is associated to each one. At each given time, a set of intersection streets where the vehicle could be located are given and an approximate position on the given streets with an error of about 10%.

DATA-ANALYSIS MODULE

The data-analysis module reads the data obtained from the sensors, and outputs the open-loop trajectory of the vehicle. It could be described as follows. An absolute initial coordinate is obtained from an external aid, such as GPS antenna or a VICS The initial heading will be computed with an history of external aid data, the signals measured by the sensors, and the maps data. A software located on a server integrates the 3D acceleration measured by inertial sensors in order to obtain a displacement in meters.

The program also detects specific gestures, given a prototype for each one of them, that are either directly sent to the map-matching module or that are used to correct the kinetic values obtained from the sensors. For instance, A mixing unit, based on a probabilistic model, would compute an estimate of the tangential velocity when the vehicle is detected to be traveling at constant velocity. For this scenario, the tangential velocity obtained from the integration of the measured acceleration would be mixed with a constant velocity. Other gestures such as stopping, turning, starting, having a constant acceleration, making a U-turn, making a full circle and so on, could be used to mix either the acceleration, velocity or the displacement computed, via integration, from the measured values of the sensors.

Remarks

1. The sensors are generally not separated in space with the analysis computer. In our system, the data-analysis computer wirelessly obtains the data from the sensors, through Cellemetry. For now, we plan to only use one 3D accelerometer.

2. As aforementioned, our system does not use any external aid other than the maps data stored on the server. That is, it does not have a second independent means, such as GPS, to determine the position, and then used to refine the position obtained through integration of the measured signals through, for example , of a Kalman filter. Our system only uses a combination of integration and gesture-matching with the raw data from the

sensors to obtain a displacement and certain gestures. We do not plan to use Kalman filters at this time.

MAP-MATCHING MODULE

Certain gestures, such as turning, and the displacement are sent to the map-matching module. Only the map-matching module provides the external aid to the data-analysis module, by defining a set of constraints that the vehicle has to obey, since the truck should only travel on known routes. The map-matching program assigns a probability to each possible branches taken by the vehicle and selects the one having the highest probability depending on the stochastic model.

Remarks

1. The module merely makes a relation between the distance traveled and the detected gestures, with the set of routes that it has possibly taken. It does not display the precise position of the vehicle but an approximate position, or set of positions, based on a stochastic model. It is worth mentioning that each position, along with its error function, is located on its own street segment.

Name	Size	Modified	Comment
15.PDF	111,606	3/24/90 9:08 AM	
10.PDF	314,969	3/24/90 9:04 AM	
11.PDF	457,017	3/24/90 9:07 AM	
12.PDF	251,391	3/24/90 9:07 AM	
13.PDF	261,587	3/24/90 9:07 AM	
14.PDF	178,950	3/24/90 9:08 AM	
1.PDF	332,908	3/24/90 9:18 AM	
16.PDF	5,546	3/24/90 9:32 AM	
17.PDF	4,056	3/24/90 9:36 AM	
18.PDF	5,324	3/24/90 9:38 AM	
19.PDF	7,359	3/24/90 9:43 AM	
2.PDF	302,077	3/24/90 8:50 AM	
20.PDF	4,453	3/24/90 9:49 AM	
3.PDF	397,059	3/24/90 8:51 AM	
4.PDF	455,531	3/24/90 8:51 AM	
5.PDF	568,256	3/24/90 8:52 AM	
6.PDF	539,114	3/24/90 8:52 AM	
7.PDF	539,107	3/24/90 9:09 AM	
8.PDF	252,298	3/24/90 9:00 AM	
9.PDF	253,911	3/24/90 9:03 AM	

Name	Size	Modified	Comment
30.PDF	7,072	3/24/90 10:10 AM	
22.PDF	6,911	3/24/90 9:38 AM	
23.PDF	4,309	3/24/90 9:49 AM	
24.PDF	247,796	3/24/90 9:51 AM	
25.PDF	92,275	3/24/90 9:52 AM	
26.PDF	7,225	3/24/90 10:00 AM	
27.PDF	8,565	3/24/90 10:01 AM	
28.PDF	50,127	3/24/90 10:02 AM	
29.PDF	21,892	3/24/90 10:02 AM	
21.PDF	10,613	3/24/90 9:43 AM	

CLAIMS

1- A method for sending selected data in a monitoring application comprising the following steps:

a) sensing for a control signal comprising control information necessary for determining how said selected data is to be sent from a remote transceiver to a base station;

b) if said control signal is sensed, transmitting said selected data using said control information and;

c) if said control signal is not sensed, transmitting said selected data a plurality of times in an attempt to increase a probability that said data reaches said base station.

2- A system for sending selected data in a monitoring application comprising:

a) means for sensing a control signal;

b) means for transmitting said selected data through using said control information in the event such control signal is present;

c) means for transmitting said selected data without using said control information in the event such control signal is not present.

3- A method for tracking the location of a cargo or of a vehicle comprising the following steps:

a) locating the initial position of the said cargo or vehicle;

b) sensing for an unauthorized movement of said cargo or vehicle;

c) if an unauthorized movement is sensed, transmission of data in relation to the motion of said cargo or vehicle;

d) if an unauthorized movement is not sensed, acquisition of data in relation to the position of said cargo or vehicle.

4 – A system for tracking the location of a cargo or of a vehicle comprising:

a) means for determining the coordinates of a first location;

b) means for detecting the unauthorized displacement of said cargo or vehicle;

c) means for measuring data in relation to the motion of said cargo or vehicle;

d) In the event an unauthorized movement is detected, transmittal of a wireless signal including said data in relation to the motion of said cargo or vehicle;

e) means for determining the coordinates of a second location using said data in relation to the motion of said cargo or vehicle.